

	COMPUTER AIDED DISPATCH (CAD) SYSTEM ACCESS	Operations Order 5.3.02
	PHOENIX POLICE DEPARTMENT	New 12/15 PAGE 1

1. GENERAL INFORMATION

- A. This policy applies to authorized personnel who access information through the Computer Aided Dispatch (CAD) system, its sub-systems, and any external systems/applications/databases, to include but not limited to, the:
- Administrative sub-system
 - Arizona Criminal Justice Information System (ACJIS)
 - Arizona Crime Information Center (ACIC)/National Crime Information Center (NCIC)
 - Arizona Department of Transportation (ADOT) Motor Vehicle Division (MVD)
 - Automatic Number Identification/Automatic Location Identification (ANI/ALI) system
 - Centrally Linked Information for Public Safety (CLIPS™) application
 - Department's records management system (RMS)
 - GEOBASE database
 - Motorola Air Traffic Information Access (ATIA) data feed
- B. Only personnel with a Terminal Operator Certification (TOC) are allowed access to the CAD system which contains confidential and personal identifying information.
- C. Fingerprint based criminal history and stringent background checks are required for all personnel who access the CAD system.
- D. The Department is considered an "interface agency" to the Arizona Department of Public Safety (DPS) and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and is therefore subject to rules and regulations imposed by those agencies.

2. CAD ACCESS

- A. Licenses - All CAD license ownership resides with the Communications Bureau.
- The CAD administrator will review and approve all requests for CAD installations based upon the business need and available licenses.
 - Approved requests for license funding and purchases will be managed by the CAD administrator and the Communications Bureau.
 - The installation location of CAD must comply with CJIS Privacy and Security policy requiring computer equipment to be maintained in a secure location to prevent access/viewing by unauthorized personnel.
- B. CAD access will be:
- Based upon the user's role within the Department.
 - Authorized based on the least privilege required to perform assigned tasks.
 - Granted only if approved by the supervisor of the user and CAD administrator or designee.
 - Authorized only if the user has undergone fingerprint based background checks (state and federal) with no criminal history that would preclude employment.
- C. All personnel authorized to access CAD must obtain a Level A, B, C, D, or E TOC issued by DPS, based on the user's role within the Department.
- NOTE:** Authorized personnel must renew their TOC every two years.
- D. CAD access is limited to law enforcement related responsibilities/duties.

	COMPUTER AIDED DISPATCH (CAD) SYSTEM ACCESS	Operations Order 5.3.02
	PHOENIX POLICE DEPARTMENT	New 12/15 PAGE 2

- 2 E. Requests – All requests for CAD access must be submitted by the user's supervisor via the Service Desk application on PolicePoint and will be processed during normal business hours by the CAD administrator or designee.

EXCEPTION: For urgent after hour requests, contact the Information Technology Bureau (ITB) Operations.

- The IT Service Desk CAD Account Request Template must include the following information:
 - * User's serial number
 - * User's network identification (ID)
 - * User's assignment /role
 - * Written authorization and business need justification by the user's supervisor
 - * Date of expiration (for temporary assignments)

- E. Transfers – When personnel are reassigned or transferred to other positions within the Department, appropriate actions such as, closing or establishing accounts and changing access authorizations, will occur upon notification of the transfer.

- F. Retirements/Terminations - Upon notification of an authorized user's retirement/termination, authorized personnel or processes will disable all user IDs.

- G. Misuse of CAD Access - The user's supervisor will determine if the misuse is a major information technology (IT) or CJIS security violation or a minor Department policy violation.

(1) Major violations will be referred to the Professional Standards Bureau (PSB) for investigation.

(2) Minor policy violations will be handled by the user's supervisor.

3. **CAD USER ACCOUNTS**

- A. A "User" account will be established for each authorized user requiring access to CAD and each account will have a unique user ID.

(1) Authorized users include:

(a) Department employees including reserve officers

(b) Non-employees:

- Interns and in some cases, consultants and contractors when start and end dates are known
- Volunteers working set hours and days for an unknown length of time

- B. The CAD system will authenticate each user's identity in a manner consistent with CAD's protection requirements.

- C. Security Groups - User accounts will be assigned a CAD security group and NCIC security group that provides access to specific commands, forms, and tools.

- * Security group assignments will be based upon employee classification, specific job duty, and/or assignment.
- * Any changes to a user's security groups must be authorized by the CAD administrator.

	COMPUTER AIDED DISPATCH (CAD) SYSTEM ACCESS	Operations Order 5.3.02
	PHOENIX POLICE DEPARTMENT	New 12/15 PAGE 3

4. **SUSPENDING USER ACCOUNTS** – A user's account will automatically be suspended after 90 days of non-use.
 - Requests to reactivate a suspended CAD account must be submitted by the user's supervisor via the Service Desk application on PolicePoint.
5. **REVIEWING ACCOUNTS** - The CAD administrator will review the database of user accounts every 90 days to ensure access remains appropriate.
 - A. Outdated or inappropriate access privileges will be revoked and documented.
 - B. A review of all CAD licenses and their bureau assignments will occur biannually or as necessary.
6. **COMPLIANCE AUDITS** – The City Auditor Department may conduct periodic audits to evaluate compliance with the requirements set forth in this order.

Last Organizational Review: